

Amendment to the Claim:

This listing of claims will replace all prior versions, and listings, of the claims in the applications.

Claim listing:

Claim 1 (Currently Amended) A detection system for identifying and eliminating excessive request for information on a network to prevent the failure of a portion of the network, comprising:

at least one switching device, wherein the switching device has predefined parameters for the receipt of an acceptable volume of requests for information;

at least one server, wherein the switching device and server are in electronic communication with each ~~together~~ other; and wherein the switching device is configured to receive requests for information and attempts to respond to the request; and

an activity monitoring system, the activity monitoring system comprising a route arbiter and a traffic analyzer, wherein the activity monitoring system is in electronic communication with the switching device.

Claim 2 (Original): A detection system as claimed in claim 1, further comprising a firewall, wherein the firewall is configured to receive requests for information.

Claim 3 (Original): A detection system as claimed in claim 1, wherein the route arbiter monitors the requests received by the router.

Claim 4 (Original): A detection system as claimed in claim 2, wherein the route arbiter is coupled to the firewall and the switching device, and wherein the route arbiter monitors the requests received by the firewall and the switching device.

Claim 5 (Original): A detection system as claimed in claim 1, wherein the route arbiter is configured to compare the volume of requests to the predefined parameters for the receipt of an acceptable volume of requests.

Claim 6 (Original): A detection system as claimed in claim 1, wherein the route arbiter is configured to instruct the switching device to direct requests for information to the traffic analyzer.

Claim 7 (Original): A detection system as claimed in claim 1, further comprising a null address router, wherein the null address router is coupled to the traffic analyzer.

Claim 8 (Original): A method for preventing the failure of a first network device on a network, wherein the network has a network address that is broadcast, and wherein the first network device is configured to receive a predefined volume threshold of packets of information from a second network device, comprising:

the first network device receiving repeated packets of information from the second network device, wherein the second network device identifies the first network device by the network address;

monitoring the volume and frequency of the transmitted packets of information;
determining whether the volume of transmitted packets of information exceeds the predefined threshold of acceptable volume of transmission of packets of information;

directing the transmission of packets of information from the second network device to an analyzer; analyzing the transmission of packets of information at the traffic analyzer; and

responding to the forwarding of the packets of information from the second network device.

Claim 9 (Original): A method as claimed in claim 8, wherein responding to the forwarding of packets of information further comprises instructing the first network to cease advertising the network address to the second network device.

Claim 10 (Original): A method as claimed in claim 8, wherein responding to the forwarding of packets of information further comprises forwarding the packets of information from the analyzer to a null address router.

Claim 11 (Original): A process for identifying and preventing the failure of a network device on a first network having a plurality of first network devices, wherein the first network is coupled to a second network via at least one edge router, the second network having a plurality of second network devices, and wherein the first network comprises a core router, a server having a server network address, a route arbiter, and a traffic analyzer, and wherein the core router announces the server network address to the second network and first network devices, comprising:

- predefining a parameter for an acceptable volume of traffic from a transmitting source;
- receiving a first volume of traffic at the core router, wherein the volume of traffic is transmitted from a first source;

- monitoring the first volume of traffic by the route arbiter;

- determining whether the first volume of traffic exceeds the predefined parameter of an acceptable volume of traffic from a transmitting source;

- if the first volume of traffic exceeds the predefined volume parameter, instructing the core router to direct the first volume of traffic from the first source to the traffic analyzer;

- analyzing the first volume of traffic to determine whether the volume is decreasing; and
- responding to the excessive volume of traffic.

Claim 12 (Original): A process as claimed in claim 11, wherein responding to the excessive volume of traffic comprises instructing the router to cease announcing the server network address to the first source.

Claim 13 (Original): A process as claimed in claim 11, wherein responding to the excessive volume of traffic comprises directing the traffic from the first source to a null address router.

Claim 14 (Original): A method for determining the best connection or path for a router to transmit traffic to a specific destination on a network, wherein a path on a network includes a

plurality of independent segments that are coupled together via links, and wherein the volume of users on the network defines the network load, comprising:

- analyzing the amount of network load; and

- analyzing link availability to determine the specific links to traverse, wherein the analysis of link availability comprises:

 - analyzing traffic load on the specific link pathway, wherein the traffic load is the volume of users on the specific link; and

 - analyzing the availability of the network.

Claim 15 (Original): A method as claimed in claim 14, wherein analyzing the traffic load on a specific pathway further comprises transmitting a sample packet from a starting point and measuring the amount of time for the packet to return to the starting point.

Claim 16 (Previously Presented): A system for identifying and eradicating fraudulent requests on a network, comprising:

- a filtering module coupled to a network;

- a verification module coupled to the filtering module;

- an anomaly recognition module coupled to the filtering module, wherein the anomaly recognition module identifies fraudulent network requests in accordance with predefined anomaly criteria;

- a protocol analysis module coupled to the filtering module, wherein the protocol analysis module identifies fraudulent network requests in accordance with predefined protocol analysis criteria; and

- a rate limiting module coupled to the filtering module, wherein the rate limiting module limits the rate of requests on a network in accordance with predefined rate limiting criteria.

Claim 17 (Previously Presented). A detection system, comprising:

- a switching device coupled to a network for providing access to network traffic, wherein the network traffic has predefined acceptable characteristics; and

an activity monitoring system coupled to the switching device.

Claim 18 (Previously Presented). The detection system of claim 16, further comprising a firewall coupled to the switching device.

Claim 19 (Previously Presented). An activity monitoring system, comprising:

a route arbiter coupled to a switching device, wherein the route arbiter monitors network activity on the switching device in accordance with predefined acceptable parameters; and

a traffic analyzer coupled to the switching device, such that the traffic analyzer redirects the network traffic in response to the route arbiter when the network activity exceeds the predefined acceptable parameters.

Claim 20 (Previously Presented). The activity monitoring system of claim 19, wherein the redirected network traffic is directed to a null address.

Claim 21 (Previously Presented). A method for validating incoming packets from a network, comprising:

detecting a predefined condition associated with the incoming packets; and

instructing a switching device to direct the incoming packets to a traffic analyzer, in accordance with the predefined condition.

Claim 22 (Previously Presented). The method of claim 21, wherein the predefined condition is associated with abnormal network activity.

Claim 23 (Previously Presented). The method of claim 22, wherein the abnormal network activity is the occurrence of a nondecreasing volume of traffic at a predefined threshold level for a predefined period of time.

Claim 24 (Previously Presented). The method of claim 21, wherein the predefined condition is associated with abnormal traffic patterns.

Claim 25 (Previously Presented). A system for preventing transmission of data on a network, comprising:

a router coupled to a network, wherein data is transmitted between the network and the router;

a server coupled to the router; and

an activity monitoring module coupled to the router, wherein the activity monitoring module monitors the transmitted data in accordance with predetermined acceptance criteria and responds in accordance with predetermined response criteria.

Claim 26 (Previously Presented). An activity monitoring system, comprising:

a route arbiter coupled to a network, wherein the route arbiter monitors activity on the network in accordance with predefined acceptance criteria, wherein the predefined acceptance criteria are used to determine whether the activity is abnormal; and

a traffic analyzer coupled to the route arbiter, wherein the traffic analyzer responds to abnormal activity determined by the route arbiter, in accordance with predefined response criteria.

Claim 27 (Previously Presented). The activity monitoring system of claim 26, wherein the route arbiter is coupled to the network via a switching device.

Claim 28 (Previously Presented). The activity monitoring system of claim 27, wherein the switching device is a router.

Claim 29 (Previously Presented). The activity monitoring system of claim 26, wherein the predefined acceptance criteria indicate whether the influx of network activity is changing in volume.

Claim 30 (Previously Presented). The activity monitoring system of claim 26, wherein the predefined acceptance criteria indicate that the network activity is not decreasing in volume, and wherein the predefined response criteria is a threshold network activity level.

Claim 31 (Previously Presented). A method for preventing transmission of data on a network, comprising:

identifying problematic data traffic on a network, in accordance with predefined traffic pattern criteria; and

processing the problematic traffic in accordance with predefined redirection criteria.

Claim 32 (Previously Presented). The method of claim 31, wherein the predefined redirection criteria cause the problematic traffic to be blocked.

Claim 33 (Previously Presented). The method of claim 31, wherein the predefined redirection criteria cause the problematic traffic to be redirected to a device that does not respond to the problematic traffic.

Claim 34 (Previously Presented). The method of claim 31, wherein the predefined redirection criteria cause the problematic traffic to be redirected to a null address.